State of Illinois

Department of Central Management Services

AVAILABILITY POLICY

Effective January 30, 2007

Public Distribution
Version 1.0

AVAILABILITY POLICY

Effective January 30, 2007

Version 1.0

APPROVAL SHEET

EXPEDITED APPROVAL

BCCS Deputy Director: _____ Date: _____

If approved digitally (via email), attach copy & write subject line & date below.

Owner: _____ Date: _____

If approved digitally (via email), attach copy & write subject line & date below.

Policy Review Board Chair: _____ Date: _____

If approved digitally (via email), attach copy & write subject line & date below.

Return to Policy Review Board Chair

Expedited publications MUST be formally submitted to the Policy Review Board within 180 days from the BCCS Deputy Director approval date in order to undergo customary review and stakeholder comment or the publication will be withdrawn and retired.

TABLE OF CONTENTS

POLICY STATEMENT

Essential and critical business functions will be available whenever needed including but not limited to a disruption in normal operations.

PURPOSE

Provide an enterprise-level strategy to ensure that all critical business functions will continue to function in the event of a disruption to normal processing.

BUSINESS CASE

Delivery of service, and ultimately Illinois citizens, will suffer if needed resources, tools, and functionality are not available. Due care and due diligence as well as best practice require that continuity of business functions be a management obligation. This requires that actions be documented and tested, and that personnel be trained to ensure that business operations will continue and can be recovered if an event occurs that disrupts normal processing.

RELEVANCE

U.S. Patriot Act,

Sec. 1016. Critical Infrastructures Protection.
(b) (3)

> A continuous national effort is required to ensure the reliable provision of cyber and physical infrastructure services critical to maintaining the national defense, continuity of government, economic prosperity, and quality of life in the United States.

Federal Information Security Management Act of 2002

§ 3544. Federal Agency Responsibilities
(b) AGENCY PROGRAM.

> Each agency shall develop, document, and implement an agency-wide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes—
>
> (1) periodic assessments of the risk and magnitude of assets of the agency;
>
> (8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

Industry standards and best practice: ISO 17799 and COBIT

SCOPE

Human safety will be the primary concern in the event of an incident and is addressed separately in an evacuation and/or incident response plan.

This policy covers enterprise-wide business operational functions and is therefore not limited to information processing activities. Recovery of source documents and manual processes, relocation of work areas (people, communications, furniture, equipment, etc.), and interaction with customers and vendors must be included in a business function continuity and recovery plan.

DEFINITIONS

The following terms are used in this policy. For additional information on a specific term, click on the term below to display its definition or find it in the Shared Services Glossary.

- *Availability*
- *Due Diligence*

ENFORCEMENT

Noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including discharge, may involve civil or criminal litigation, and may involve financial assessment, restitution, fines, or penalties.

RESPONSIBILITY

Each business unit manager is responsible for ensuring that essential manual and automated business functions, processes, inputs, outputs, reports, etc can be recovered and will continue in the event normal operations are interrupted.

Business unit managers are responsible for testing a business continuity and recovery plan and ensuring that appropriate personnel are trained on proper recovery procedures.

Business unit managers are responsible for informing their staff of the necessity to input and schedule changes in the organization's change management system to avoid potential conflicts and to alert the enterprise to potential down time.

Business unit managers are responsible for participating in a risk assessment evaluation to rank their business process at an enterprise level and to identify areas of risk that can be mitigated.

Individual staff are responsible for following organizational policy and procedure, for practicing due diligence, and for assisting or participating in any pertinent recovery effort.

POLICY

An enterprise change management process will be established that involves and informs all appropriate parties (staff and vendors) of changes that could possibly cause a disruption to normal processing.

Each business unit will construct, publish, and test a business recovery plan that conforms to enterprise standards and will, at a minimum, include actions to recognize, react, remediate, relocate, resume/reconstruct, and return as defined in current standards.

An enterprise business continuity and recovery plan will be published comprised of all business unit recovery plans and will not be limited to information processing.

Any personnel, internal staff or vendor staff, may be selected to participate in the recovery process and may be assigned specific responsibility as part of their overall job duties or contractual obligation.

The plan and/or sections of the plan will be validated (rehearsed, exercised, tested) at least annually (validation options include and are limited to those sanctioned by the Disaster Recovery Institute International).

REVISION HISTORY

Created: May 1, 2006
Revised: Nov 13, 2006 / June 26, 2006 / 12/18/2006
Reviewed: Nov 13, 2006
Effective: Jan 30, 2007

- End of Availability Policy -